International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 2, Apr 2014, 205-212

TRANS STELLAR
• Journal Publications • Research Consultancy

STUDY AND COMPARISON OF CRYPTOGRAPHIC METHODS FOR CLOUD SECURITY

ASHWINI BANGAR & SWAPNIL SHINDE

Department of Information Technology, RAIT, Nerul, Mumbai, Maharashtra, India

ABSTRACT

Cloud Computing is an emerging technology widely used in the IT sector due its wide range of characteristics. These characteristics serve a medium for the intruders to attack the cloud and its users. The security of cloud can be compromised by employing different strategies and techniques. Many systems and techniques have been proposed for solving the security issues and implementing a high level of security on both the sides. Encryption is one of the best method suggested for making the cloud more secure and increasing its areas of application. This paper contains an overall study and comparison of various cryptographic algorithms implemented for cloud security. We also study some hybrid systems designed using combination of various crypto terminologies for enhancing data security in cloud. The hybrid systems implement multiple cryptographic algorithms like RSA and Digital signature, Diffie Hellman and AES in combination with Digital signature. Some of the comparison parameters included are technique proposed, type of algorithm, algorithm, scalability.

KEYWORDS: AES, DES, Diffie Hellman, Digital Signature, Encryption

INTRODUCTION

Cloud computing [6] is a buzzword that means different things to different people. For some, it's just another way of describing IT (information technology) "outsourcing", others use it to mean any computing service provided over the Internet or a similar network; and some define it as any bought-in computer service you use that sits outside your firewall. It may be broadly categorized as software-as-a-service, platform-as-a-service and infrastructure-as-a-service. PaaS (Platform as a Service) - offer specific applications too, such as Google App Engine in combination with Google Docs. Examples: Force.com, Google App Engine, Windows Azure (Platform). Infrastructure as a Service (IaaS) also referred to as Resource Clouds, provide (managed and scalable) resources as services to the user. Accordingly, different resources may be provided via a service interface. Software as a Service (SaaS), also sometimes referred to as Service or Application Clouds are offering implementations of specific business functions and business processes that are provided with specific cloud capabilities, i.e. they provide applications / services using a cloud infrastructure or platform, rather than providing cloud features themselves. Often, kind of standard application software functionality is offered within a cloud.

Deployment Models

Private Clouds are typically owned by the respective enterprise and / or leased. Functionalities are not directly exposed to the customer, though in some cases services with cloud enhanced features may be offered – this is similar to (Cloud) Software as a Service from the customer point of view. Example: eBay

Public Clouds: Enterprises may use cloud functionality from others, respectively offer their own services to users outside of the company. Providing the user with the actual capability to exploit the cloud features for his / her own purposes also allows other enterprises to outsource their services to such cloud providers, thus reducing costs and effort to build up their own infrastructure. As noted in the context of cloud types, the scope of functionalities thereby may differ. Example: Amazon, Google Apps, Windows Azure.

Hybrid Clouds: Hybrid clouds consist of a mixed employment of private and public cloud infrastructures so as to achieve a maximum of cost reduction through outsourcing whilst maintaining the desired degree of control over e.g. sensitive data by employing local private clouds.

Community Clouds: Typically cloud systems are restricted to the local infrastructure, i.e. providers of public clouds offer their own infrastructure to customers. Though the provider could actually resell the infrastructure of another provider, clouds do not aggregate infrastructures to build up larger, cross-boundary structures. In particular smaller SMEs could profit from community clouds to which different entities contribute with their respective (smaller) infrastructure. Community clouds can either aggregate public clouds or dedicated resource infrastructures.

Cryptography [10] is the art and science of protecting information from undesirable individuals by converting it into a form non-recognizable by its attackers while stored and transmitted. Data cryptography mainly is the scrambling of the content of data, such as text, image, audio, video and so forth to make the data unreadable, invisible or unintelligible during transmission or storage called Encryption. The main goal of cryptography [11] is keeping data secure form unauthorized attackers. In this paper we will be studying how security issues related to cloud computing can be overcome by using various cryptographic algorithms. The paper comprise of a comparison between various cryptographic algorithms which includes some parameters like.

SECURITY ISSUES IN CLOUD [7]

- **Authentication and Identity Management:** By using cloud services, users can easily access their personal information and make it available to various services across the Internet. An identity management (IDM) mechanism can help authenticate users and services based on credentials and characteristics.
- **Access Control and Accounting:** It's important that the access control system employed in clouds is easily managed and its privilege distribution is administered efficiently. We must also ensure that cloud delivery models provide generic access control interfaces for proper interoperability, which demands a policy-neutral access control specification and enforcement framework that can be used to address cross-domain access issues.
- **Trust Management and Police Integration:** In cloud computing environments, the interactions between different service domains driven by service requirements can be dynamic, transient, and intensive. Thus, a trust framework should be developed to allow for efficiently capturing a generic set of parameters required for establishing trust and to manage evolving trust and interaction/sharing requirements.
- **Secure-Service Management:** Although many cloud service providers use the Web Services Description Language (WSDL), the traditional WSDL can't fully meet the requirements of cloud computing services description. In clouds, issues such as quality of service, price, and SLAs are critical in service search and composition. These issues must be addressed to describe services and introduce their features, find the best

interoperable options, integrate them without violating the service owner's policies, and ensure that SLAs are satisfied.

- **Privacy and Data Protection:** By migrating workloads to a shared infrastructure, customers' private information faces increased risk of potential unauthorized access and exposure. Cloud service providers must assure their customers and provide a high degree of transparency into their operations and privacy assurance. Privacy-protection mechanisms must be embedded in all security solutions.
- **Organizational Security Management:** The information security area has faced significant problems in establishing appropriate security metrics for consistent and realistic measurements that help risk assessment. We must reevaluate best practices and develop standards to ensure the deployment and adoption of secure clouds. These issues necessitate a well-structured cyber insurance industry, but the global nature of cloud computing makes this prospect extremely complex.

TYPES OF CRYPTOSYSTEM

The types of crypto system are as follows:

- Symmetric(private) key cryptography
- Asymmetric(public)key cryptography
- Hash Functions

Symmetric Key system involves use of single key for encryption and decryption. It has mainly two categories stream cipher and block cipher [1]. Some of the most well known block cipher include DES, AES and stream cipher include RC4.

DES [5] is block cipher used for encryption of 64 bit block using a 56 bit key. It includes a key generation block and round function which contains many operations like permutation, expansion, substitution and Xoring. There are 16 rounds in DES where a new key is generated for each round. The DES was advanced to double DES and 3DES [1][5] by increasing the size of the key for improving the security. AES is block cipher with variable key size of 128,192 or 256 applied on same size blocks using rounds varying from 10 to 14.

In terms of Asymmetric key system RSA [5] is most widely used algorithm for encryption purpose along with Diffie Hellman key exchange and Digital signatures. RSA can be Summarized as follows:

Choose two prime numbers, 'p' and 'q'. From these numbers you can calculate the modulus, n = pxq. Select a third number 'e' that is relatively prime to the product (p-l) (q-l). The number 'e' is the public exponent. Calculate an integer 'd' from the quotient (ed-l) / [(p-l) (q-l)]. The number 'd' is the private exponent. The public key pair is(n,e) and private key pair is (n,d). Hash Functions are also called message digest are used to maintain the integrity of the message while it is transferred via a medium. Hash functions[5] are one way and they generate a hash value that is unique and is irreversible. Mostly used hash functions are SHA, MD5 and Tiger hash respectively.

PROPOSED TECHNIQUES: STUDY

One of the simplest examples of a substitution cipher is the Caesar cipher [2]. It is said to have been used by Julius Caesar to communicate with his army. Caesar is considered to be one of the first persons to have ever employed encryption for the sake of securing messages. Caesar decided that shifting each letter three places down the alphabet in the message would be his standard algorithm, and so he informed all of his generals of his decision, and was then able to send them secured messages. One of the strengths of the Caesar cipher is its ease of use and this ease of use would be important for

Caesar since his soldiers were likely uneducated and not capable of using a complicated coding system. Further enhancement to original three places shifting of character in Caesar cipher uses modulo twenty six arithmetic [5] encryption key that is greater than twenty six.

$$En(x) = (x+n) \bmod 26$$

The most pressing weakness of this cipher is simplicity of its encryption and decryption algorithms; the system can be deciphered without knowing the encryption key. It is easily broken by reversing encryption process with simple shift of alphabet ordering [11].

$$Dn(x) = (x-n) \bmod 26$$

The earliest ceaser cipher method include the main drawbacks is plaintext and key is used only 26 alphabets. The paper by Dr. A. Padmapriya et al[] overcomes the above problem, the plaintext used is case sensitive, numbers and special characters in order of ASCII full characters (256 char). This proposed method providing the inverse of Caesar cipher that supports more security for the data compared with the earliest Caesar cipher. And also it can be used simply encode the message for preserving privacy. It is complicated to understand the cipher text compared with the other methods.

Algorithm Procedure

Step 1: Get the plaintext from the user (Ei) E-Encrypted text, i Text length.

Step 2: Get the key value from the range numbers (0 to 256) (Ki) K-Key value, i Key length.

Step 3: Apply the formula Ei (X+K) Mod 256 or Ei (X+K) – 256.

Step 4: Decryption Ei (X-K) Mod 256 or Ei (X-K) – 256.

RSA is widely used Public-Key algorithm. RSA stands for Ron Rivest, Adi Shamir and Len Adleman, who first publicly described it in 1977. In proposed work by Kalpana parsi et al[3], RSA algorithm is used to encrypt the data to provide security so that only the concerned user can access it. By securing the data unauthorized access is blocked. User data is encrypted first and then it is stored in the Cloud. When required, user places a request for the data for the Cloud provider, Cloud provider authenticates the user and delivers the data. RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only. RSA algorithm involves three steps:

- Key Generation
- Encryption
- Decryption

In Cloud computing, we have problem like security of data, files system, backups, network traffic, and host security. Here Neha Jain et al[1] proposed system for data security using encryption decryption with DES algorithm while we are transferring it over the network. The Data Encryption Standard (DES) is the name of the Federal Information Processing Standard (FIPS) 46-3, Which Describes the data encryption algorithm (DEA). The DES has been extensively studied since its publication and is the most widely used symmetric algorithm in the world. The DES has a 64-bit block size key during execution. DES is a symmetric cryptosystem, specifically a 16-round Feistel Cipher. When used for communication, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message, or to generate and verify a Message Authentication Code (MAC). The DES can also be used for Single-user encryption, such as to store files on a hard disk in encrypted form.The DES has a 64-bit block size and uses a 56 bit key during execution.

In Cipher Block Chaining mode of operation of DES, each block of ECB encrypted cipher text is XO Red with the next plain text block to be encrypted, thus making all the blocks dependent on all the previous blocks. This means that in order to find the plaintext of a particular block, you need to know the cipher text, the key and the cipher text for the previous bIock. The first block to be encrypted has no previous cipher text, so the plaintext is XO Red with a 64-bit number called the initialization vector (referred as IV).So if data is transmitted over network or phone line and there is a transmission error, the error will be carried forward to all the subsequent blocks since each block is dependent upon the last. This mode of operation is more secure than ECB (electronic code book) because the extra XOR step adds one more layer to the encryption process.

Compositions of Encryption and Decryption

Encryption E = eL1 o eL2 ..... o eL16

Decryption D = dL16 o dL15 o .....o dL1

Steps

Get the Plaintext.

Get the Password.

Convert the Characters into binary form.

Derive the Leaders (L1 to L16) from the Password.

Apply the Formula to get the encrypted and decrypted message

Security using third party or third resource is widely used in many areas. The third party acts as a secure medium for exchange of data and storing of data. Kerberos is one of the authentication protocol used for trusted third party implementation in terms of information and data security. It has its own set of rules that are applied for authentication and access of the server side information.

Cloud also implements client server architecture for providing its services to its user providing high level of security. One of the method proposed by Prasad Rewagad et al[4] uses a three way mechanism, where the security is increased to great extent. The step wise uploading of a file is done in three steps as follows:

- Diffie hellman generates keys for key exchange
- Once key exchange is done then digital signature authenticates the user
- AES is used for encrypting the file and then it is stored in storage server

Second server is used for encryption purpose and there is key generation repository for Exchange process. Exact reverse procedure is done to download the file from the storage server.

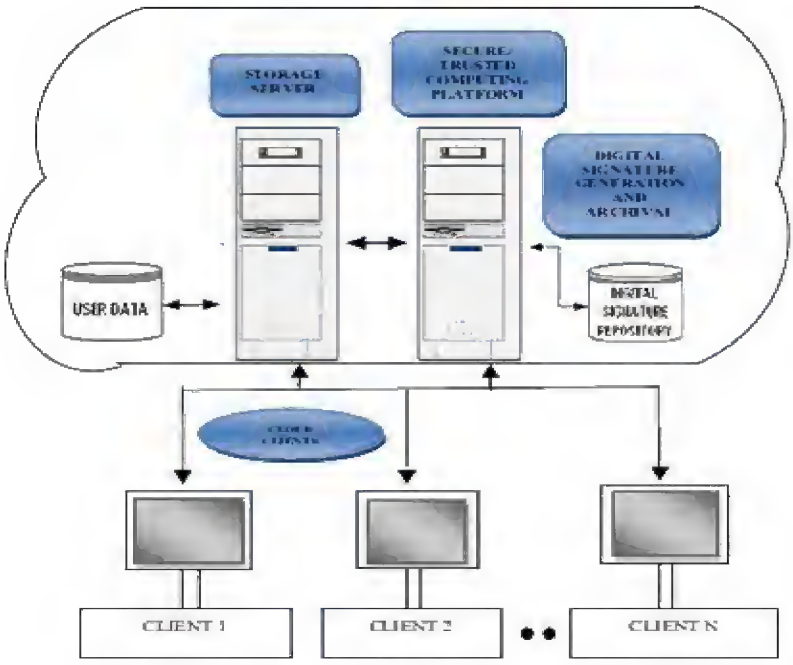

Figure 1

Cloud security challenges gives rise to need for new techniques to enhance the data security in cloud computing environment. Cloud Computing has a virtual environment that enables transfer of data to the cloud users. This transfer should be more secure and reliable so it should satisfy the three main goals of security: Confidentiality, integrity and availability.

Paper proposed by Uma Somani et al[5] satisfies main goals of security providing a very high and efficient level of security.

The Proposed system can be explained in the following steps:

Step 1: Select the file/ document requested by the user

Step 2: Apply Hash function to generate the message digest

Figure 2

Step 3: This message digest wil be encrypted to create a digital signature which will be used for authentication

Figure 3

Step 4: RSA algorithm is used and digitally signed message digest is encrypted by public key then transferred.

COMPARISON

Table 1

Sr. No.	Technique Proposed	Type of Cryptography	Algorithm	Scalability	Security Applied to	Authentication Method
1	Reverse Ceaser Cipher for Data Security	Substitution Cipher	Reverse Ceaser	Scalabale	User Data	Substitution applied
2	Data Security using RSA algorithm	Asymmetric	RSA	Not scalable	Client Side only	Robust authentication applied
3	Implementing DES algorithm for Cloud Data Security	Symmetric	DES	Scalable due to variable key size	Both Providers and Client side	Message Authentication
4	Digital Signature and RSA for Data security	Asymmetric	RSA	Scalable	Client side only	Digital signature, Message authentication
5	Diffie Hellman, Digital Signature and RSA for Enhanching Data Security	Asymmetric and Key Exchange	RSA and Diffie Hellman	Not scalable	Client side only	Digital signature, Message authentication

CONCLUSIONS

The Cloud computing is growing technology and is increasing rapidly with the development of IT. In Cloud computing technology there are a set of important rules and regulations that are to be followed which include issues of privacy, security, anonymity, telecommunications capacity, government surveillance, reliability among others. Data security is a major concern in the cloud environment. Virtual cloud environment provides a lot of scope for the intruders to attack the cloud data and the user data. Generally, Cloud computing has several customers such as ordinary users, academia, and

enterprises who have different motivation to move to cloud. If cloud clients are academia, security effect is on performance of computing and for them cloud provides a way to combine security and performance. For enterprises the most important problem is also security but with different vision. For them high performance may be not as critical as academia. The security level changes from type of the user and the cloud designed for its implementation. An overall study of various cloud security concepts is done in this paper. The focus of paper is on for enhancing the security of cloud. Both symmetric and study n comparison of various cryptography algorithms implemented asymmetric type of cryptography techniques have been used for encryption of user data along with different authentication methods applied to each of them. RSA, Diffie Hellman, DES, AES are some of the cryptographic algorithms applied maintain the data security in cloud and many parameters are used for their comparison.

REFERENCES

1. Neha Jain and 2Gurpreet Kaur, 'Implementing DES Algorithm in Cloud for Data Security', VSRD-IJCSIT, Vol. 2 (4), 2012, 316-321.
2. Dr. A. Padmapriya and P. Subhasri, 'Cloud Computing: Reverse Caesar Cipher Algorithm to Increase Data Security', IJETT – Volume 4 Issue 4- April 2013
3. Parsi Kalpana and Sudha Singaraju, 'Data Security in Cloud Computing using RSA Algorithm', IJRCCT, ISSN 2278-5841, Vol 1, Issue 4, September 2012.
4. Prashant Rewagad and Yogita Pawar, 'Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing', 2013 IEEE – ICCSNT
5. Uma Somani, Kanika Lakhani, Manish Mundra, 'Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing', 2010 IEEE – ICPDGC
6. Introduction to Cloud Computing white paper Dialogic, 2010
7. Pradeep Kumar Tiwari and Dr. Bharat Mishra, "Cloud Computing Security Issues, Challenges and Solution", IJETAE, Volume 2, Issue 8, August 2012.
8. Hassan Takabi, James B. D. Joshi and Gail-Joon Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE, November/December 2010.
9. Thoran Rodrigues, "Cloud Security: Technology, Processes, Responsibility", The Enterprise Cloud, May 29, 2012.
10. Thai Duong and Juliano Rizzo, 'Cryptography in the Web: The Case of Cryptographic Design Flaws in ASP.NET', 2011 IEEE.
11. Diffie, W. and Hellman, M.E., 'New directions in cryptography', IEEE 1976, ISSN - 0018-9448, Volume: 22, Issue: 6.